JOURNAL OF COMBINATORIAL THEORY, Series A **62**, 139–154 (1993)

M.D.S. Codes and Arcs in $PG(n, q)$ with q Even: An Improvement of the Bounds of Bruen, Thas, and Blokhuis

L. STORME* AND J. A. THAS

Seminar of Geometry and Combinatorics, University of Ghent, Krijgslaan 281, B-9000 Gent, Belgium

Communicated by Francis Buekenhout

Received October 1, 1990

All bounds of Bruen, Thas, and Blokhuis in [*Invent. Math.* **92** (1988), 441–459] are considerably improved: we show that $\sqrt[3]{q}$ may be replaced by $\sqrt{q}/2 + 3/4$.

1. INTRODUCTION

Let $\Sigma = PG(n, q)$ denote the n-dimensional projective space over the field $GF(q)$. A k-arc of points in Σ (with $k \geqslant n+1$) is a set K of points with the property that no $n+1$ points of K lie in a hyperplane. Sometimes it is more convenient to discuss matters in terms of the dual object: A k-arc of hyperplanes, again $k \geqslant n+1$, is a set of hyperplanes no $n+1$ of which pass through a point. We say that a k-arc of Σ is complete if it cannot be extended to a $(k+1)$-arc of Σ.

It is well known [2] that k-arcs of $PG(n, q)$ and linear M.D.S. codes (Maximum Distance Separable codes) of dimension $n+1$ and length k over $GF(q)$, are equivalent objects. Hence any result on k-arcs can be translated in terms of linear M.D.S. codes, and conversely. The k-arcs which correspond with generalized Reed–Solomon codes and generalized doubly extended Reed–Solomon codes are subsets of normal rational curves [8].

In 1955, B. Segre posed the following problems [7]:

(1) For given n and q what is the maximum value of k for which there exist k-arcs in $PG(n, q)$?

(2) For what values of n and q, with $q > n+1$, is every $(q+1)$-arc of $PG(n, q)$ the point set of a normal rational curve?

* Senior Research Assistant of the National Fund for Scientific Research (Belgium).

0097-3165/93 $5.00

582a/62/1-10

(3) For given n and q, with $q > n+1$, what are the values of k for which every k-arc of $PG(n, q)$ is contained in a normal rational curve of this space?

2. Sketch of Known Results for q Odd [2, 10]

THEOREM 2.1 (B. Segre). *For any k-arc in $PG(n, q)$, with $q \neq 3$ and $n = 2$, 3, or 4, we have $k \leqslant q+1$; for any k-arc of $PG(n, 3)$ with $n = 2, 3$, or 4, we have $k \leqslant n+2$. For any n the point set of a normal rational curve is a $(q+1)$-arc. For $n = 2$, 3 the converse is true, i.e., a $(q+1)$-arc of $PG(2, q)$ is an irreducible conic and a $(q+1)$-arc of $PG(3, q)$ is a twisted cubic.*

THEOREM 2.2 (J. A. Thas). (a) *For any k-arc of $PG(n, q)$, $q > (4n - 23/4)^2$, we have $k \leqslant q+1$.*

(b) *In $PG(n, q)$, with $q > (4n - 23/4)^2$, every $(q+1)$-arc is the point set of a normal rational curve.*

(c) *In $PG(n, q)$ every k-arc with $k > q - \sqrt{q}/4 + n - 7/16$ is contained in one and only one normal rational curve of this space.*

Remarks. 1. By a recent note due to H. Kaneta and T. Maruta [6] the bound in (a) of Theorem 2.2 can be improved to $q > (4n - 39/4)^2$.

2. By a result of J. F. Voloch [11], combined with the note mentioned in Remark 1, for q a prime the bounds in (a), (b), (c) of Theorem 2.2 can be respectively improved to $q > 45n - 140$, $q > 45n - 95$, and $k > 44q/45 + n - 10/9$.

3. D. G. Glynn proves that in $PG(4, 9)$ there exists a 10-arc which is not a normal rational curve.

3. Sketch of Known Results for q Even [2, 10]

In $PG(2, q)$, q even, it is easy to show that for a k-arc we have $k \leqslant q+2$ and that $(q+2)$-arcs exist.

THEOREM 3.1 (B. Segre). *A k-arc of $PG(2, q)$ with $k > q - \sqrt{q} + 1$ is contained in a $(q+2)$-arc; for $q > 2$ this $(q+2)$-arc is unique and for $q = 2$ there are two such 4-arcs. For any n the point set of a normal rational curve is a $(q+1)$-arc.*

THEOREM 3.2 (J. C. Fisher, J. W. P. Hirschfeld, and J. A. Thas; E. Boros and T. Szönyi). *For any square q, complete $(q - \sqrt{q} + 1)$-arcs exist in $PG(2, q)$.*

THEOREM 3.3 (L. R. A. Casse). *For any k-arc of* $PG(3, q)$, $q>2$, *we have* $k \leqslant q+1$; *for any k-arc of* $PG(3, 2)$ *we have* $k \leqslant 5$. *For any k-arc of* $PG(4, q)$, $q>4$, *we have* $k \leqslant q+1$; *for any k-arc of* $PG(4, 2)$ *or* $PG(4, 4)$ *we have* $k \leqslant 6$.

THEOREM 3.4 (L. R. A. Casse and D. G. Glynn). *Every* $(q+1)$*-arc of* $PG(3, q)$, $q=2^h$, *is projectively equivalent to*

$$C=\{(1, t, t^e, t^{e+1}) \mid t \in GF(q) \cup \{\infty\}\},$$

where $e=2^m$ *and* $(m, h)=1$. *Any* $(q+1)$*-arc of* $PG(4, q)$ *is a normal rational curve.*

THEOREM 3.5 (H. Kaneta and T. Maruta [6]). *For any k-arc of* $PG(5, q)$, $q>4$, *we have* $k \leqslant q+1$; *for any k-arc of* $PG(5, 2)$ *or* $PG(5, 4)$ *we have* $k \leqslant 7$.

THEOREM 3.6 (J. A. Thas). *For any k-arc in* $PG(q-2, q)$ *there holds* $k \leqslant q+2$ *and a* $(q+2)$*-arc can be constructed by adjoining to a normal rational curve a certain point, its nucleus.*

THEOREM 3.7 (A. A. Bruen, J. A. Thas, and A. Blokhuis). (a) *Let K be a k-arc of* $PG(3, q)$, $q \neq 2$. *If* $k \geqslant q+3-\sqrt[3]{q}$, *then K can be completed to a* $(q+1)$*-arc which is uniquely determined by K.*

(b) *In* $PG(n, q)$, $n \geqslant 4$ *and* $q \geqslant (n-2)^3$, *there holds* $k \leqslant q+1$ *for every k-arc K.*

(c) *In* $PG(n, q)$, $n \geqslant 4$ *and* $q \geqslant (n-1)^3$, *every* $(q+1)$*-arc is a normal rational curve.*

(d) *Let K be a k-arc in* $PG(n, q)$, $n \geqslant 4$, $q=2^h$, $h \geqslant 2$ *and* $k \geqslant q+n-\sqrt[3]{q}$. *Then K lies in a normal rational curve L of* $PG(n, q)$. *Moreover L is completely determined by K.*

Remark. The main new idea introduced in [2] was to associate to each k-arc of hyperplanes in $PG(3, q)$ and $PG(4, q)$, with q even, a hypersurface of degree $q+3-k$, resp. $q+4-k$, and to use the properties of these hypersurfaces, combined with the proof of Theorem 2.2, to obtain Theorem 3.7. In [1] a hypersurface of degree $q+n-k$, resp. $2(q+n-k)$, is associated to each k-arc of hyperplanes of $PG(n, q)$, q even, resp. q odd.

4. Duality Principle for k-Arcs

Theorem 4.1 (J. A. Thas [9]). *A k-arc of $PG(n, q)$, $n \geqslant 2$ and $k \geqslant n+4$, exists if and only if a k-arc of $PG(k-2-n, q)$ exists. For $n \geqslant 2$ and $k \geqslant n+4$ we have:*

$$\frac{\text{number of } k\text{-arcs of } PG(n, q)}{\text{number of } k\text{-arcs of } PG(k-n-2, q)} = \frac{\text{number of normal rational curves of } PG(n, q)}{\text{number of normal rational curves of } PG(k-n-2, q)}.$$

Corollary. *If every $(q+1)$-arc of $PG(n, q)$, $n \geqslant 2$ and $q \geqslant n+3$, is a normal rational curve, then every $(q+1)$-arc of $PG(q-1-n, q)$ is a normal rational curve.*

Remark. In terms of M.D.S. codes the first part of Theorem 4.1 tells us that the dual code of a linear M.D.S. code is again a linear M.D.S. code.

5. Improvement of the Bounds in $PG(3, q)$, q Even

Let $K = \{\pi_1, \pi_2, ..., \pi_k\}$ be a k-arc of planes in $PG(3, q)$, q even, and assume that $k > q - \sqrt{q} + 2$. If Φ is the surface of degree $q+3-k$ associated to K, then by Lemma 1.5 of [2] each curve $\Phi \cap \pi_i = C_i$ of degree $t = q+3-k$ factors into t lines which form an arc of lines in the plane π_i. These t lines $L_{i1}, L_{i2}, ..., L_{it}$ together with the lines $\pi_i \cap \pi_j$, $i \neq j$ and $1 \leqslant i, j \leqslant k$, form a $(q+2)$-arc of lines in π_i. The lines $L_{i1}, L_{i2}, ..., L_{it}$ are called S-lines or Segre lines. We note that any S-line lies in a unique plane of K. By Lemma 1.6 of [2] each point p lying on an S-line lies on exactly one other S-line.

Lemma 5.1. *If $q - \sqrt{q}/2 + 9/4 < k < q+1$, then for any plane π of $PG(3, q)$ the curve $\Phi \cap \pi$ is reducible over the algebraic closure $\bar{\gamma}$ of $\gamma = GF(q)$.*

Proof. Clearly $k > q - \sqrt{q} + 2$ and since there is an integer between $q - \sqrt{q}/2 + 9/4$ and $q+1$, we necessarily have $q \geqslant 32$.

We may assume that no S-line is contained in π. Then any S-line has exactly one point in common with π. Since the number of S-lines is equal to $k(q+3-k) = kt$ and each point is on either 0 or 2 S-lines, we have

$$|\Phi \cap \pi| \geqslant kt/2.$$

Assume $\Phi \cap \pi$ is absolutely irreducible, i.e., irreducible over $\bar{\gamma}$. By the Hasse–Weil bound we then have

$$(q+3-k)k/2 \leqslant q+1+(q+2-k)(q+1-k)\sqrt{q}.$$

Consequently, either $k \geqslant q+1$ or $k \leqslant q-\sqrt{q}/2+9/4-1/(4+8\sqrt{q}) < q-\sqrt{q}/2+9/4$, a contradiction. We conclude that $\Phi \cap \pi$ is reducible over $\bar{\gamma}$. ∎

LEMMA 5.2. *If $q-\sqrt{q}/2+9/4 < k < q+1$ and k is even, then for each plane π of $PG(3, q)$ the curve $\Phi \cap \pi = C$ contains a line as component (over γ).*

Proof. We may assume that no S-line is contained in π. By Lemma 5.1 the curve C is reducible over $\bar{\gamma}$. We have $2 < t < \sqrt{q}/2+3/4$ and $q \geqslant 32$.

If C' is an absolutely irreducible component of C of degree m, with $m \geqslant 4$, then we show that $|C'| < (q+1)m/2$.

If C' is not defined over γ, then $|C'| \leqslant m^2$ [5, p. 221]; if C' is defined over γ, then by the Hasse–Weil bound $|C'| \leqslant q+1+(m-1)(m-2)\sqrt{q}$. Since $q+1+(m-1)(m-2)\sqrt{q} \geqslant m^2$, we always have $|C'| \leqslant q+1+(m-1)\times(m-2)\sqrt{q}$. Assume that

$$q+1+(m-1)(m-2)\sqrt{q} \geqslant (q+1)\,m/2.$$

Then either

$$\frac{\sqrt{q}}{4}+\frac{3}{2}+\frac{1}{4\sqrt{q}}+\frac{1}{4}\sqrt{(\sqrt{q}-2)^2+2-\frac{4}{\sqrt{q}}+\frac{1}{q}} \leqslant m$$

or

$$\frac{\sqrt{q}}{4}+\frac{3}{2}+\frac{1}{4\sqrt{q}}-\frac{1}{4}\sqrt{(\sqrt{q}-2)^2+2-\frac{4}{\sqrt{q}}+\frac{1}{q}} \geqslant m.$$

Hence either

$$m > \frac{\sqrt{q}}{4}+\frac{3}{2}+\frac{\sqrt{q}-2}{4} = \frac{\sqrt{q}}{2}+1$$

or

$$m < \frac{\sqrt{q}}{4}+\frac{3}{2}+\frac{1}{4\sqrt{q}}-\frac{\sqrt{q}-2}{4} = 2+\frac{1}{4\sqrt{q}}.$$

This contradicts $4 \leqslant m < t < \sqrt{q}/2+3/4$. Hence $|C'| < (q+1)m/2$.

If C'' is an absolutely irreducible component of C of odd degree m, with $m \geqslant 5$, then we show that $|C''| < ((m-3)/2)(q+1) + q + 1 + 2\sqrt{q}$. Note that by the Hasse–Weil bound $q+1+2\sqrt{q}$ is the maximum number of points of an absolutely irreducible plane cubic curve over γ.

If C'' is not defined over γ, then $|C''| \leqslant m^2$; if C'' is defined over γ, then $|C''| \leqslant q+1+(m-1)(m-2)\sqrt{q}$. Hence always $|C''| \leqslant q+1+(m-1)(m-2)\sqrt{q}$. Since $5 \leqslant m \leqslant q+1-k < \sqrt{q}/2 - 5/4$ we have $q \geqslant 256$. Assume that

$$\frac{m-3}{2}(q+1)+q+1+2\sqrt{q} \leqslant q+1+(m-1)(m-2)\sqrt{q}.$$

Then either

$$m \leqslant \frac{\sqrt{q}}{4} + \frac{1}{4\sqrt{q}} + \frac{3}{2} - \frac{1}{4}\sqrt{(\sqrt{q}-6)^2 + 2 - \frac{12}{\sqrt{q}} + \frac{1}{q}}$$

or

$$m \geqslant \frac{\sqrt{q}}{4} + \frac{1}{4\sqrt{q}} + \frac{3}{2} + \frac{1}{4}\sqrt{(\sqrt{q}-6)^2 + 2 - \frac{12}{\sqrt{q}} + \frac{1}{q}}.$$

Since $q \geqslant 256$ we have $2 - 12/\sqrt{q} + 1/q > 0$. Hence either

$$m < \frac{\sqrt{q}}{4} + \frac{3}{2} + \frac{1}{4\sqrt{q}} - \frac{\sqrt{q}-6}{4} = 3 + \frac{1}{4\sqrt{q}}$$

or

$$m > \frac{\sqrt{q}}{4} + \frac{3}{2} + \frac{\sqrt{q}-6}{4} = \frac{\sqrt{q}}{2}.$$

This contradicts $5 \leqslant m < \sqrt{q}/2 - 5/4$, and so $|C''| < ((m-3)/2)(q+1) + q+1+2\sqrt{q}$.

Assume that C contains no linear component over γ, but contains $\beta (\geqslant 0)$ linear components over $\bar{\gamma}$. Since C has odd degree, the number of components (over $\bar{\gamma}$) of C of odd degree is odd. By the preceding sections and using $2(q+1+2\sqrt{q}) < 3(q+1)$ we now have

(i) for β even $|C| \leqslant \dfrac{t-\beta-3}{2}(q+1) + \beta + (q+1+2\sqrt{q})$

$$\leqslant \frac{t-3}{2}(q+1) + q + 1 + 2\sqrt{q};$$

(ii) for β odd $|C| \leqslant \dfrac{t-\beta}{2}(q+1) + \beta < \dfrac{t-3}{2}(q+1) + q + 1 + 2\sqrt{q}$.

Hence always

$$|C| \leqslant \frac{t-3}{2}(q+1)+q+1+2\sqrt{q}.$$

Consequently

$$\frac{k(q+3-k)}{2} \leqslant |C| \leqslant \frac{q-k}{2}(q+1)+q+1+2\sqrt{q}.$$

So, either

$$k \leqslant q+2-\sqrt{(\sqrt{q}-3)^2+2\sqrt{q}-7}$$

or

$$k \geqslant q+2+\sqrt{(\sqrt{q}-3)^2+2\sqrt{q}-7}.$$

Hence either

$$k < q+2-(\sqrt{q}-3) = q-\sqrt{q}+5$$

or

$$k > q+2+(\sqrt{q}-3) = q+\sqrt{q}-1.$$

This contradicts

$$q-\frac{\sqrt{q}}{2}+\frac{9}{4} < k < q+1.$$

We conclude that C contains a line as component over γ. ∎

THEOREM 5.3. *If* $q-\sqrt{q}/2+9/4 < k < q+1$ *and* k *is even, then* Φ *contains a plane as component* (*over* γ).

Proof. Let π_i be a plane of the k-arc. In π_i there are $q+3-k = t < \sqrt{q}/2+3/4$ S-lines which form an arc of lines in π_i. Since $q \geqslant t(t-3)/2+2$, this arc is incomplete, so there is a line which intersects the t lines of the arc at t different points [5, p. 205]. Hence $|L \cap \Phi| = t$ and the t points of $\Phi \cap L$ are simple for Φ. Considering the $q+1$ planes of $PG(3, q)$ through L and using Lemma 5.2, we see that at least one point p of $\Phi \cap L$ is contained in at least $(q+1)/t$ lines of Φ. Hence p is contained in at least $2\sqrt{q}-4+(\sqrt{q}/2+4)/(\sqrt{q}/2+3/4)$ lines of Φ. It follows that the tangent plane π_p of Φ at p contains more than $2\sqrt{q}-4$ lines of Φ. Since $2\sqrt{q}-4 > t$ the plane π_p is a component of Φ. ∎

THEOREM 5.4. *Any k-arc K of $PG(3,q)$, with q even, k even and $q-\sqrt{q}/2+9/4<k<q+1$, can be extended to a $(k+1)$-arc.*

Proof. This follows immediately from Theorem 1.3 of [2] and Theorem 5.3. ∎

LEMMA 5.5. *If $q-\sqrt{q}/2+9/4<k<q+1$ and k is odd, then for each plane π of $PG(3,q)$ the curve $\Phi\cap\pi=C$ either contains a line as component over , or consists of $t/2$ irreducible conics defined over γ.*

Proof. We may assume that no S-line is contained in π.

If C' is an absolutely irreducible component of C of degree m, with $q+2-k>m>4$ and $q>512$, then we show that $|C'|<((m-4)/2)(q+1)+q+1+2\sqrt{q}$. Note that by the Hasse–Weil bound $q+1+2\sqrt{q}$ is the maximum number of points of an absolutely irreducible plane cubic curve over γ.

Ignore at the moment the condition $q>512$. If C' is not defined over γ, then $|C'|\leqslant m^2$; if C' is defined over γ, then $|C'|\leqslant q+1+(m-1)(m-2)\sqrt{q}$. Hence always $|C'|\leqslant q+1+(m-1)(m-2)\sqrt{q}$. Since $5\leqslant m\leqslant q+1-k<\sqrt{q}/2-5/4$ we have $q\geqslant 256$. Assume that

$$\frac{m-4}{2}(q+1)+q+1+2\sqrt{q}\leqslant q+1+(m-1)(m-2)\sqrt{q}. \tag{1}$$

Then either

$$m\leqslant\frac{\sqrt{q}}{4}+\frac{3}{2}+\frac{1}{4\sqrt{q}}-\frac{1}{4}\sqrt{(\sqrt{q}-11)^2+2\sqrt{q}-\frac{20}{\sqrt{q}}+\frac{1}{q}-83}$$

or

$$m\geqslant\frac{\sqrt{q}}{4}+\frac{3}{2}+\frac{1}{4\sqrt{q}}+\frac{1}{4}\sqrt{(\sqrt{q}-11)^2+2\sqrt{q}-\frac{20}{\sqrt{q}}+\frac{1}{q}-83}.$$

For $q>1024$ we have $2\sqrt{q}-20/\sqrt{q}+1/q-83>0$. Hence for $q>1024$ either

$$m<\frac{\sqrt{q}}{4}+\frac{3}{2}+\frac{1}{4\sqrt{q}}-\frac{\sqrt{q}-11}{4}=\frac{17}{4}+\frac{1}{4\sqrt{q}}$$

or

$$m>\frac{\sqrt{q}}{4}+\frac{3}{2}+\frac{\sqrt{q}-11}{4}=\frac{\sqrt{q}}{2}-\frac{5}{4}.$$

This contradicts $5 \leqslant m < \sqrt{q}/2 - 5/2$. For $q = 256$ the inequality (1) is satisfied; for $q = 512$ (1) together with $5 \leqslant m \leqslant q + 1 - k < \sqrt{q}/2 - 5/4$ gives $m = 10$ and $k = 503$; for $q = 1024$ (1) is in contradiction with $5 \leqslant m < \sqrt{q}/2 - 5/4$.

Let C'' be an absolutely irreducible component of degree 4 of C. If C'' is not defined over γ, then $|C''| \leqslant 16 < 2(q+1)$; if C'' is defined over γ, then $|C''| \leqslant q + 1 + 6\sqrt{q}$, and consequently $|C''| \leqslant 2(q+1)$ (for $q \geqslant 32$). Hence always $|C''| \leqslant 2(q+1)$.

Now assume that over $\bar{\gamma}$ C neither contains a line, nor consists entirely of irreducible conics and irreducible quartic curves. Assume also that $q \notin \{256, 512\}$. Let β be the number of absolutely irreducible components of degree 3, and let α be the number of absolutely irreducible components of degree at least 5. If $\alpha = 0$ then, since $q + 3 - k = t$ is even, β is even and so $\alpha + \beta$ is even. Also $\alpha + \beta > 0$. By the preceding sections

$$|C| \leqslant \frac{t - 3\beta - 4\alpha}{2}(q+1) + (\alpha + \beta)(q + 1 + 2\sqrt{q}).$$

Further note that $2(q + 1 + 2\sqrt{q}) < 3(q+1)$. If $\alpha + \beta$ is odd, so $\alpha \neq 0$, then

$$|C| \leqslant \frac{t - \alpha - 3}{2}(q+1) + q + 1 + 2\sqrt{q} \leqslant \frac{t-4}{2}(q+1) + q + 1 + 2\sqrt{q}.$$

If $\alpha + \beta$ is even, so $\alpha + \beta \geqslant 2$, then

$$|C| \leqslant \frac{t - \alpha - 6}{2}(q+1) + 2(q + 1 + 2\sqrt{q}) \leqslant \frac{t-6}{2}(q+1) + 2(q + 1 + 2\sqrt{q}).$$

So in both cases

$$|C| \leqslant \frac{t-6}{2}(q+1) + 2(q + 1 + 2\sqrt{q}) = \frac{q - k - 3}{2}(q+1) + 2(q + 1 + 2\sqrt{q}).$$

Consequently

$$\frac{k(q + 3 - k)}{2} \leqslant \frac{t-6}{2}(q+1) + 2(q + 1 + 2\sqrt{q}).$$

So, either

$$k \leqslant q + 2 - \sqrt{2q - 8\sqrt{q} + 3}$$

or

$$k \geqslant q + 2 + \sqrt{2q - 8\sqrt{q} + 3}.$$

This contradicts $q-\sqrt{q}/2+9/4<k<q+1$. Hence for $q\notin\{256, 512\}$ C contains over $\bar{\gamma}$ either a linear component, or consists entirely of absolutely irreducible conics and absolutely irreducible quartic curves.

Let C consist of ζ absolutely irreducible conics and δ absolutely irreducible quartic curves, with $\delta\geqslant 1$. If $q=32$, then $t=3$, so k is even. Hence $q\geqslant 64$. Since

$$\begin{aligned}\frac{t-4\delta}{2}&(q+1)+\delta(q+1+6\sqrt{q})\\ &=\frac{q+3-k}{2}(q+1)+\delta(-q-1+6\sqrt{q})\\ &\leqslant\frac{q+3-k}{2}(q+1)-q-1+6\sqrt{q},\end{aligned}$$

we have

$$\frac{k(q+3-k)}{2}\leqslant|C|\leqslant\frac{q+3-k}{2}(q+1)-q-1+6\sqrt{q}.$$

Consequently, either

$$k\leqslant q+2-\sqrt{2q-12\sqrt{q}+3}$$

or

$$k\geqslant q+2+\sqrt{2q-12\sqrt{q}+3}.$$

This contradicts

$$q-\frac{\sqrt{q}}{2}+\frac{9}{4}<k<q+1.$$

So over $\bar{\gamma}$, and with $q\notin\{256, 512\}$, C either contains a line or consists entirely of irreducible conics.

Let L be a line of C, and suppose that L is not defined over γ. Then $|L|\leqslant 1$. Let π_i be a plane of K not passing through a point of L over γ. The line $M=\pi\cap\pi_i$ intersects $\pi_i\cap\Phi$, and so Φ, only in points over γ. Hence the intersection of L and M is a point over γ, a contradiction.

Now suppose that C consists of $t/2$ absolutely irreducible conics, ρ of which are not defined over γ, with $\rho\geqslant 1$. Then

$$\begin{aligned}\frac{k(q+3-k)}{2}\leqslant|C|&\leqslant\frac{q+3-k-2\rho}{2}(q+1)+4\rho\\ &\leqslant\frac{q+1-k}{2}(q+1)+4.\end{aligned}$$

Hence either

$$k \leqslant q+2-\sqrt{2q-5} \qquad \text{or} \qquad k \geqslant q+2+\sqrt{2q-5},$$

a contradiction.

Consequently for $q \notin \{256, 512\}$ C either contains a line over γ or consists of $t/2$ absolutely irreducible conics over γ.

Let $q=512$. Then (1) together with $5 \leqslant m \leqslant q+1-k<\sqrt{q}/2-5/4$ gives $m=10$ and $k=503$. So assume that $m=10$ and $t=12$. If C does not contain a line, then

$$\frac{kt}{2}=\frac{503.12}{2} \leqslant |C| \leqslant (q+1)+(q+1+72\sqrt{q})=1026+72\sqrt{512},$$

a contradiction. Now, in the same way as for $q \notin \{256, 512\}$ we see that C contains a linear component over the ground field γ. If $q=512$ and if there is no absolutely irreducible component with $m>4$, then we proceed as in the case $q \notin \{256, 512\}$ with $\alpha=0$ and $\alpha+\beta=\beta \geqslant 2$.

Finally, let $q=256$. From $2<t<\sqrt{q}/2+3/4$ with t even, and $4<m<t-1$ follows that $t=8$ and $m \in \{5, 6\}$. If $t=8$, $m=5$, and C does not contain a line, then

$$\frac{kt}{2}=\frac{251.8}{2} \leqslant |C| \leqslant (q+1+12\sqrt{q})+(q+1+2\sqrt{q})=738,$$

a contradiction; if $t=8$, $m=6$ and C does not contain a line, then

$$\frac{kt}{2}=\frac{251.8}{2} \leqslant |C| \leqslant (q+1+20\sqrt{q})+(q+1)=834,$$

a contradiction. In the same way as for $q \notin \{256, 512\}$ we see that C contains a linear component over the ground field γ. If $q=256$ and if there is no absolutely irreducible component with $m>4$, then we proceed as in the case $q \notin \{256, 512\}$ with $\alpha=0$ and $\alpha+\beta=\beta \geqslant 2$. ▮

THEOREM 5.6. *If $q-\sqrt{q}/2+9/4<k<q+1$ and k is odd, then Φ contains a plane as component (over γ) or consists of $(q+3-k)/2$ hyperbolic quadrics (over γ).*

Proof. If Φ contains a plane ζ as component, then for each plane π_i of K the line $\zeta \cap \pi_i$ is an S-line, so ζ contains at least k lines over γ and consequently ζ is defined over γ.

From now on we assume that Φ does not contain a linear component. By the proof of Theorem 5.3 there is at least one plane which does not contain a line of Φ.

Let π be a plane for which $\Phi \cap \pi = C$ consists of $t/2$ irreducible conics (over γ). First we show that no two of these conics coincide.

Assume that at least two of the conics coincide. Then we have

$$\frac{k(q+3-k)}{2} \leqslant |C| \leqslant \frac{q+1-k}{2}(q+1).$$

So either

$$k \leqslant q+2-\sqrt{2q+3}$$

or

$$k \geqslant q+2+\sqrt{2q+3}.$$

This contradicts $q-\sqrt{q}/2+9/4<k<q+1$. Hence the $t/2$ conics are different.

The number of points common to at least two of these conics is at most

$$4 \cdot \frac{t}{2}\left(\frac{t}{2}-1\right)\Big/2 = \frac{t(t-2)}{2} < \frac{1}{2}\left(\frac{\sqrt{q}}{2}+\frac{3}{4}\right)\left(\frac{\sqrt{q}}{2}-\frac{5}{4}\right) < \frac{q}{8}.$$

Let C_1 be one of the conics and let p be a point of π, with $p \notin C_1$ and p distinct from the nucleus (or kernel) of C_1. Then there is at least one line L of π through p which neither contains a point over γ of C_1 nor contains a point over $\bar{\gamma}$ common to at least two conics. For this line L each point of $\bar{L} \cap \bar{\Phi}$ is a simple point for Φ. Over γ we have $|L \cap \Phi| \leqslant t-2 < \sqrt{q}/2-5/4$. Since Φ does not contain a linear component, at each point of $\bar{L} \cap \bar{\Phi}$ the tangent plane of Φ contains at most t different lines of Φ. Hence each point of $L \cap \Phi$ is contained in at most t lines of Φ. Consequently the number of planes π' through L for which $\pi' \cap \Phi$ contains a line as component over γ is at most $(t-2)t < (\sqrt{q}/2-5/4)(\sqrt{q}/2+3/4) = q/4-\sqrt{q}/4-15/16 < q/4-\sqrt{q}/4$. It follows that for more than $q+1-q/4+\sqrt{q}/4 > 3q/4+\sqrt{q}/4$ planes π' through L the curve $\Phi \cap \pi'$ consists (over γ) of $t/2$ absolutely irreducible conics. Hence over $\bar{\gamma}$ the two conjugate points in the set $\bar{L} \cap \bar{C}_1$ are contained in more than $(3q+\sqrt{q})/4$ absolutely irreducible conics of Φ, all defined over γ and lying in different planes through L. Let $C_1, C_2, \ldots,$ be these conics, and let ζ_j be the plane of C_j.

For any S-line L_i, let t_i be the number of conics of $\{C_1, C_2, \ldots\} = V$ containing at least (and then exactly one) point of L_i. The number of points of $\zeta_j \cap \Phi$ not belonging to an S-line is at most $(t/2)(q+1)-tk/2 = t(t-2)/2 < (1/2)(\sqrt{q}/2+3/4)(\sqrt{q}/2-5/4) < q/8-\sqrt{q}/8$. Hence the number of points of C_j belonging to an S-line is more than $q+1-q/8+\sqrt{q}/8 > 7q/8+\sqrt{q}/8$. As each point of Φ is on 0 or 2 S-lines it now follows that

$$\sum_i t_i > \frac{(3q+\sqrt{q})}{4} \cdot \frac{(7q+\sqrt{q})}{8} \cdot 2 = \frac{21q^2+10q\sqrt{q}+q}{16}. \tag{2}$$

The number of S-lines is equal to $(q+3-k)k$. Since the function $f(x)=(q+3-x)x$ is strictly decreasing for $x \geqslant (q+3)/2$, we have

$$(q+3-k)k < \left(\frac{\sqrt{q}}{2}+\frac{3}{4}\right)\left(q-\frac{\sqrt{q}}{2}+\frac{9}{4}\right)=\frac{q\sqrt{q}}{2}+\frac{q}{2}+\frac{3\sqrt{q}}{4}+\frac{27}{16}. \quad (3)$$

From (2) and (3) it now follows that

$$\bar{t}=\left(\sum_i t_i\right)\Big/((q+3-k)k) > \frac{21q^2+10q\sqrt{q}+q}{8q\sqrt{q}+8q+12\sqrt{q}+27} > \frac{21}{8}\sqrt{q}-2.$$

Hence there is an S-line N which has a point in common with more than $21\sqrt{q}/8-2$ conics of the set V, say with $C_1, C_2, ..., C_s$.

The common points of $C_1, C_2, ..., C_s$ are denoted by y and y'. Remind that y, y' are conjugate points over $\bar{\gamma}$. Let r_i be the common point of N and C_i, with $i=2, 3$, and let M_2, M_2' be the tangent lines of C_2 at the respective points y, y'. The (absolutely irreducible) quadric (over γ) containing C_1, r_2, r_3 and having M_2, M_2' as tangent lines will be denoted by Q. Since $r_2 \in Q$ and since the tangent lines M_2, M_2' of C_2 are tangent lines of Q, the conic C_2 belongs to Q. Since N has at least three points in common with Q, it also belongs to Q. The common point of N and C_i will be denoted by r_i and the tangent lines of C_i at the respective points y, y' will be denoted by M_i, M_i', with $i=1, 2, ..., s$. The tangent plane of Φ, respectively Q, at the point y (respectively y') is the plane M_1M_2 (respectively $M_1'M_2'$). Hence the tangent lines $M_i=M_1M_2 \cap \zeta_i$, $M_i'=M_1'M_2' \cap \zeta_i$ of C_i are also tangent lines of Q, $i=3, 4, ..., s$. Since moreover $r_i \in Q$, the conic C_i belongs to Q, $i=3, 4, ..., s$. Consequently the s conics $C_1, C_2, ..., C_s$ belong to Q. As $2s > 21\sqrt{q}/4-4 > 2t$ we have $Q \subset \Phi$ by the theorem of Bezout.

By taking for C_1 any other conic of $\Phi \cap \pi$ we then see that Φ consists of $t/2$ absolutely irreducible quadrics over γ. For any plane $\pi_i \in K$ the curve $\pi_i \cap \Phi$ consists of t different S-lines, and so necessarily π_i contains exactly two different lines of any of the $t/2$ quadrics. It follows that any of the quadrics contains at least $2k > 2q-\sqrt{q}+9/2$ lines, hence is hyperbolic.

We conclude that Φ either contains a plane as component (over γ) or consists of $(q+3-k)/2$ hyperbolic quadrics (over γ). ∎

THEOREM 5.7. *Any k-arc K of $PG(3, q)$, with q even, k odd and $q-\sqrt{q}/2+9/4 < k < q+1$, can be extended to a $(k+1)$-arc.*

Proof. By Theorem 5.6 Φ contains a plane as component (over γ) or consists of $(q+3-k)/2$ hyperbolic quadrics (over γ).

If Φ contains a plane as component (over γ), then by Theorem 1.3 of [2] K can be extended to a $(k+1)$-arc.

Now assume that Φ consists of $t/2$ hyperbolic quadrics (over γ). Then we can use the proof of Theorem 2.3 in [2], and conclude that K can be extended to a $(k+1)$-arc. ▮

THEOREM A. *Let K be any k-arc (of points or planes) in $PG(3, q)$, q even and $q \neq 2$. Assume that $k > q - \sqrt{q}/2 + 9/4$. Then K can be completed to a $(q+1)$-arc $\bar{K}$. Moreover $\bar{K}$ is uniquely determined by K.*

Proof. Assume that $q - \sqrt{q}/2 + 9/4 < k < q+1$. By Theorems 5.4 and 5.7 the k-arc K is not complete and so it extends to a $(k+1)$-arc K'. If $k+1 = q+1$ we are done. If $k+1 < q+1$ then, since $k+1 > q - \sqrt{q}/2 + 9/4$ the arc K' extends to a $(k+2)$-arc K''. Proceeding in this way we get that K can be extended to a $(q+1)$-arc $\bar{K}$. By Theorem 1.4 of [2], $\bar{K}$ is uniquely determined by K since $q - \sqrt{q}/2 + 9/4 > (q+4)/2$. ▮

6. IMPROVEMENT OF THE BOUNDS IN $PG(n, q)$, q EVEN AND $n \geqslant 4$

First of all, Theorems 3.3 and 3.4 of [2] hold when $k \geqslant q + 4 - \sqrt[3]{q}$ is replaced by $k > q - \sqrt{q}/2 + 13/4$.

THEOREM 6.1. *Let K be any k-arc (of points or solids) in $PG(4, q)$, q even, with $q - \sqrt{q}/2 + 13/4 < k < q$. Then K can be extended to a q-arc of $PG(4, q)$.*

Proof. Use the proof of Theorem 4.1 in [2]. Then we have only to show that Case 2, i.e.,

$$t \geqslant ((k-1)(t-4)/(t-2) + (2t-4))/(t-1) \tag{4}$$

cannot occur for $4 < t < 3/4 + \sqrt{q}/2$. Since $4 < t < 3/4 + \sqrt{q}/2$ we necessarily have $q \geqslant 128$. By Case 2 of Theorem 4.1 in [2] we may assume that $\sqrt[3]{q} < t < \sqrt{q}/2 + 3/4$.

First, let $q = 128$. Then $t = 6$, $k = 126$. With these values of q, t, k, Eq. (4) is not satisfied. Now let $q > 128$. By (4) we have

$$t^3 - 4t^2 + 3t - qt + 4q + 4 \geqslant 0. \tag{5}$$

Hence

$$t^3 - qt + 3\left(\frac{\sqrt{q}}{2} + \frac{3}{4}\right) - 4(\sqrt[3]{q})^2 + 4q + 4 > 0.$$

Since

$$\frac{3\sqrt{q}}{2} - 4(\sqrt[3]{q})^2 + \frac{25}{4} < 0,$$

we have

$$t^3 - qt + 4q > 0.$$

But $t^3 - qt + 4q < 0$ for any t satisfying $\sqrt[3]{q} < t < \sqrt{q}/2 + 3/4$, giving a contradiction. Hence Case 2 cannot occur. ▮

THEOREM 6.2. *Any q-arc in $PG(4, q)$, q even and $q \geq 64$, can be extended to a $(q+1)$-arc in $PG(4, q)$.*

Proof. See proof of Theorem 4.2 in [2]. ▮

THEOREM B. *Let K be a k-arc (of points or hyperplanes) in $PG(4, q)$, q even and $q \neq 2$. If $k > q - \sqrt{q}/2 + 13/4$ then K can be completed to a normal rational curve $\bar{K}$. Moreover, $\bar{K}$ is uniquely determined by K.*

Proof. Since $k > q - \sqrt{q}/2 + 13/4$ there holds $q \neq 4$. By Theorem 3.4 we have $k \leq q+1$ for $q > 4$, so $k > q - \sqrt{q}/2 + 13/4$ implies $q \geq 32$ and $k \geq 33$. If $q > q - \sqrt{q}/2 + 13/4$, then $q \geq 64$. Then using Theorems 6.1 and 6.2 along with Theorem 3.4 and using that, in $PG(4, q)$, any normal rational curve is uniquely determined by any 7 of its points, the proof of Theorem B is complete. ▮

THEOREM C. *Let K be a k-arc of $PG(n, q)$, $q = 2^h$, $q \neq 2$, $n \geq 4$ and $k > q - \sqrt{q}/2 + n - 3/4$. Then K lies in a normal rational curve $\bar{K}$ of $PG(n, q)$. Moreover $\bar{K}$ is completely determined by K.*

Proof. See proof of Theorem 5.1 in [2]. ▮

THEOREM D. *In $PG(n, q)$, $q = 2^h$, $n \geq 4$ and $q > (2n - 7/2)^2$, every $(q+1)$-arc is a normal rational curve.*

Proof. See proof of Corollary 5.2 in [2]. ▮

THEOREM E. *For any k-arc K in $PG(n, q)$, q even, $n \geq 4$ and $q > (2n - 11/2)^2$, we have $k \leq q+1$.*

Proof. See proof of Corollary 5.3, Part (2), in [2]. ▮

7. DUALITY

Applying the duality principle of 4 to Theorems C to E, we obtain

THEOREM F. (a) *In $PG(r, q)$, $q - 4 \geq r > q - \sqrt{q}/2 - 11/4$ and $q = 2^h$, there holds $k \leq q+1$ for every k-arc K.*

(b) *In* $PG(r, q)$, $q-5 \geqslant r > q-\sqrt{q}/2-11/4$ *and* $q=2^h$, *every* $(q+1)$-*arc is a normal rational curve.*

(c) *Let* K *be a k-arc in* $PG(r, q)$, $r > q-\sqrt{q}/2-11/4$, $q=2^h$, $q \neq 2$, *and* $k \geqslant 6+r$. *Then* K *lies in a normal rational curve* $\bar{K}$ *of* $PG(r, q)$. *Moreover* $\bar{K}$ *is completely determined by* K.

REFERENCES

1. A. BLOKHUIS, A. A. BRUEN, AND J. A. THAS, Arcs in $PG(n, q)$, M.D.S. codes and three fundamental problems of B. Segre—some extensions, *Geom. Dedicata* **35** (1990), 1–11.
2. A. A. BRUEN, J. A. THAS, AND A. BLOKHUIS, On M.D.S. codes, arcs in $PG(n, q)$ with q even, and a solution of three fundamental problems of B. Segre, *Invent. Math.* **92** (1988), 441–459.
3. A. A. BRUEN, J. A. THAS, AND A. BLOKHUIS, M.D.S. codes and arcs in projective space, I. *C. R. Math. Rep. Acad. Sci. Canada* **10** (1988), 225–230.
4. A. A. BRUEN, J. A. THAS, AND A. BLOKHUIS, M.D.S. codes and arcs in projective space, II, *C. R. Math. Rep. Acad. Sci. Canada* **10** (1988), 233–235.
5. J. W. P. HIRSCHFELD, "Projective Geometries over Finite Fields," Clarendon, Oxford, 1979.
6. H. KANETA AND T. MARUTA, An elementary proof and an extension of Thas' theorem on k-arcs, *Math. Proc. Cambridge Philos. Soc.* **105** (1989), 459–462.
7. B. SEGRE, Curve razionali normali e k-archi negli spazi finiti, *Ann. Mat. Pura Appl.* **39** (1955), 357–379.
8. G. SEROUSSI AND R. M. ROTH, On M.D.S. extensions of generalized Reed–Solomon codes, *IEEE Trans. Inform. Theory* **IT-32** (1986), 349–354.
9. J. A. THAS, Connection between the Grassmannian $G_{k-1;n}$ and the set of k-arcs of the Galois space $S_{n,q}$, *Rend. Mat. (6)* **2** (1969), 121–134.
10. J. A. THAS, Projective geometry over a finite field, *in* "Handbook of Incidence Geometry" (F. Buekenhout, Ed.), North-Holland, Amsterdam, to appear.
11. J. F. VOLOCH, Arcs in projective planes over prime fields, *J. Geom.* **38** (1990), 198–200.